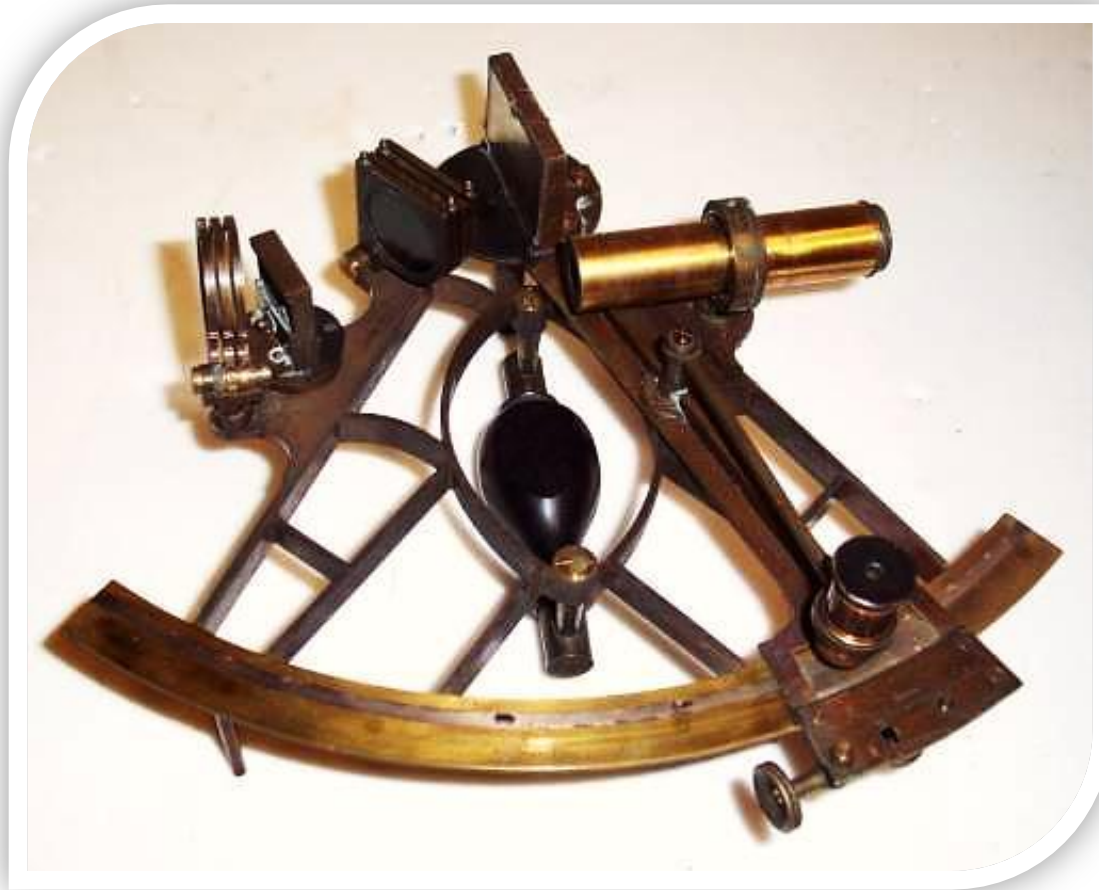




**First a test.**

**Can you...**

# Navigate with this?



# Find your container...



## *...without a computer?*



# Load your ship...



## *...without a computer?*



# Maintain fluidity ...without automation?

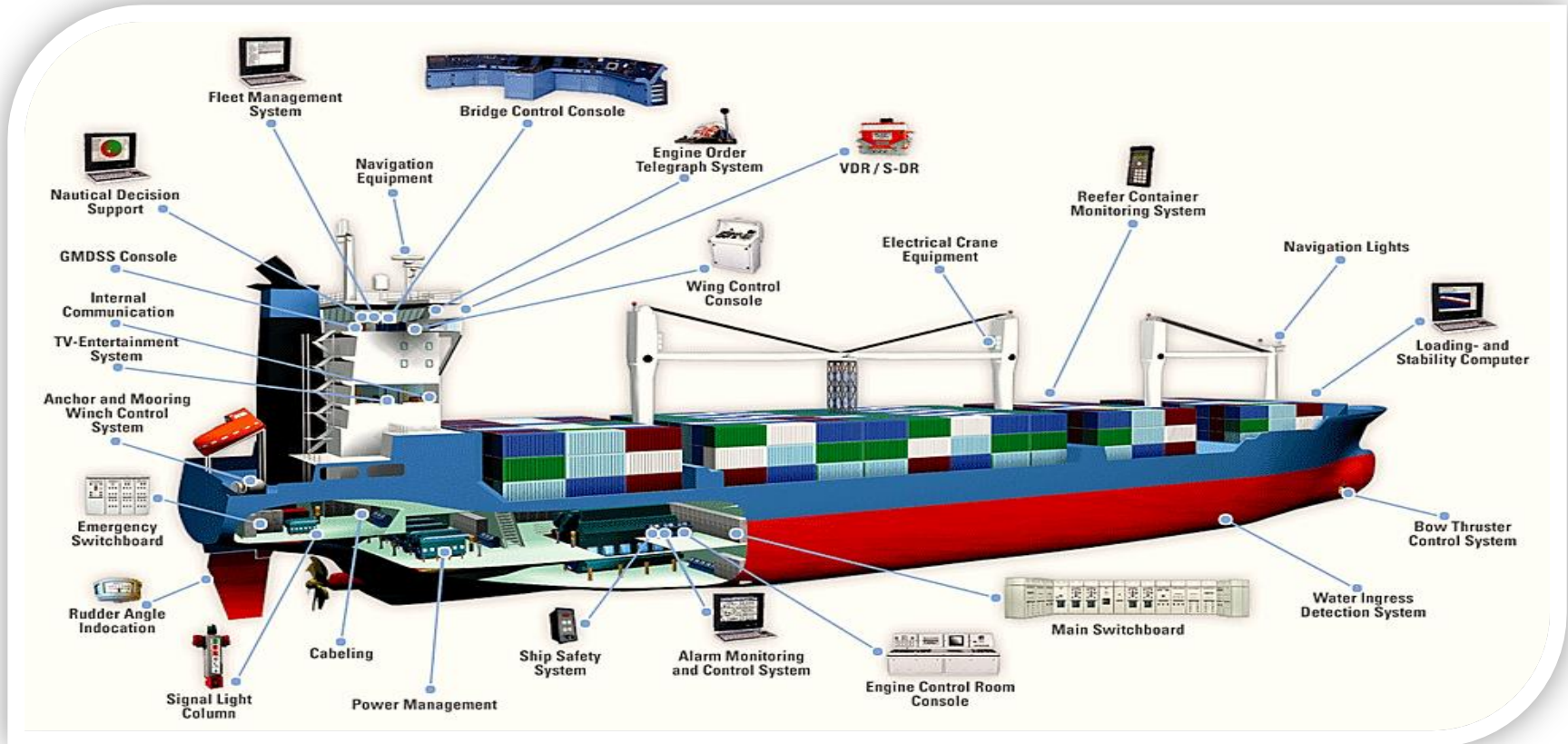


# If not, you need to pay attention to cyber security because...





# Dependent on IT & control systems when afloat





# Dependent on IT & control systems when ashore

Cargo handling  
equipment

Container  
cranes

Shore-based  
safe vessel  
operation  
systems  
(i.e. GPS, locks and  
dams, etc.)



Port security  
and access  
controls

Commercial  
trucks

Automated  
cargo handling  
equipment

Cargo tracking  
systems

Terminal  
Operating  
Center

# Cyber attacks have targeted maritime supply chains



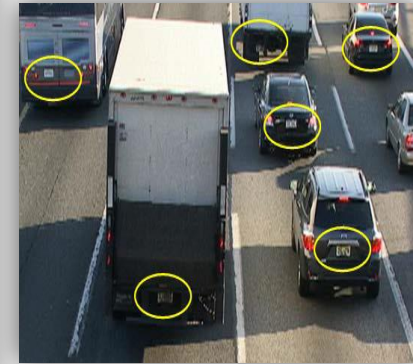
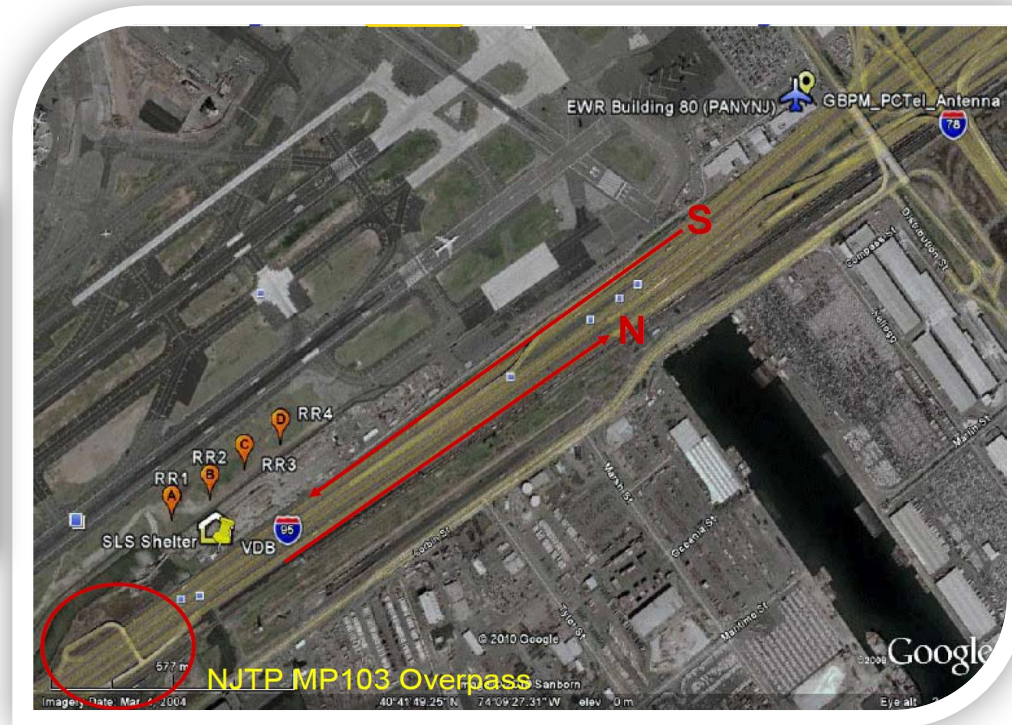
Employee awareness and security controls are critical



Coordination of cyber and physical security is key



# GPS is vulnerable to jamming & spoofing



**June 19, 2014:** The FCC issues its largest fine in history (**\$34.9M**) to a company selling signal jammers.

# Cyber security requires a life-cycle approach

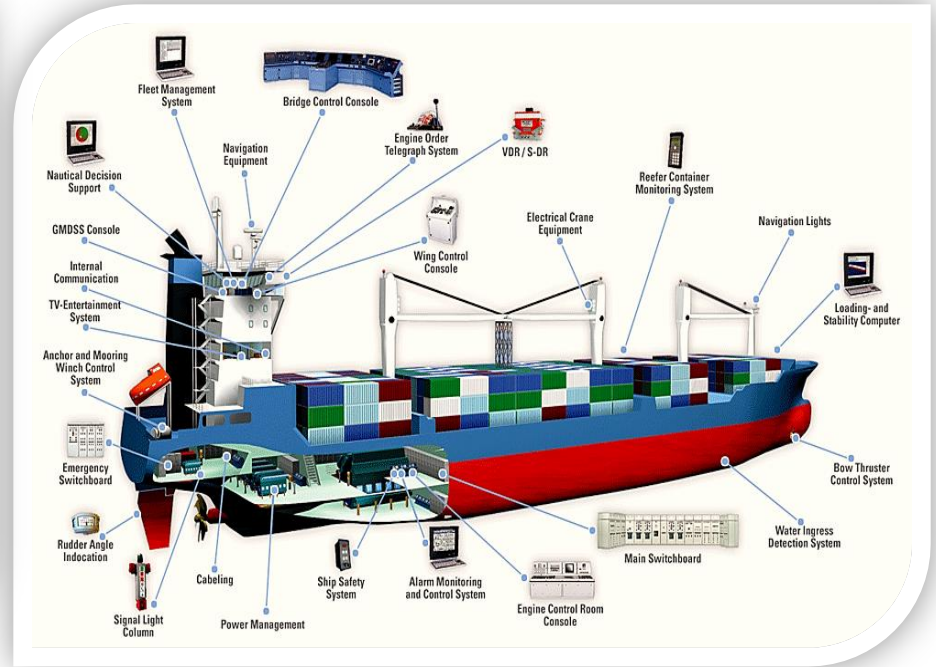
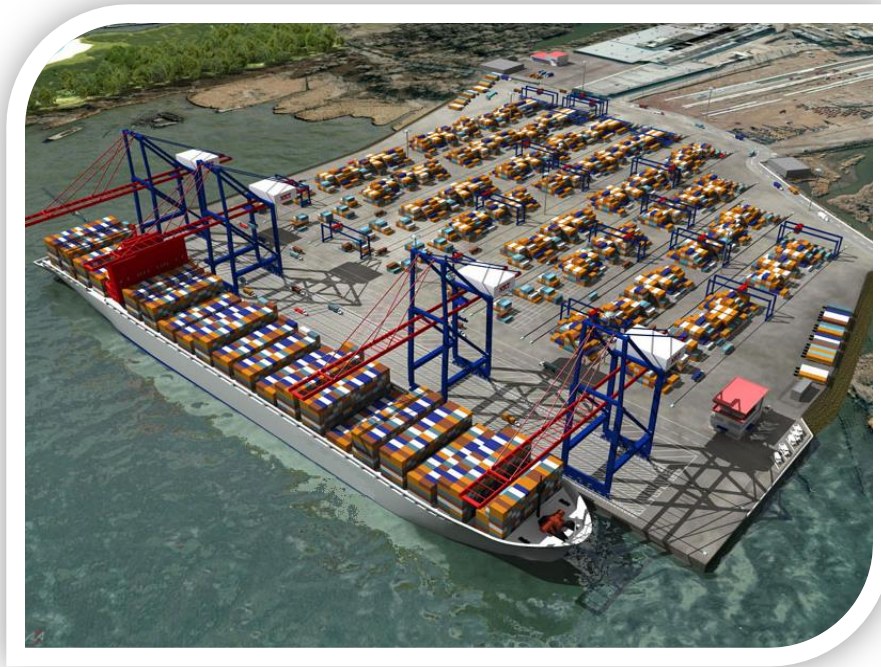




# Best practices in other modes

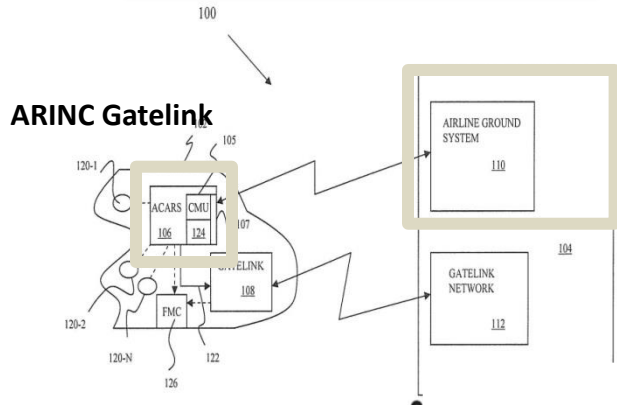


# What are the vulnerabilities & risks?



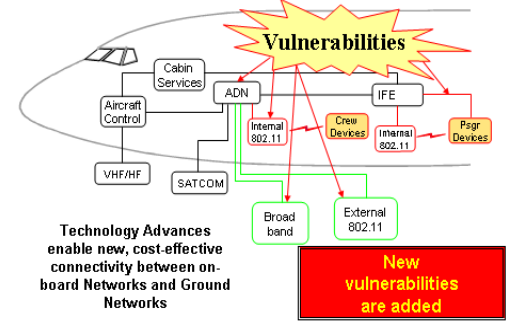
# Example: identifying vulnerabilities in aviation

## Airport Controls Systems (CS)

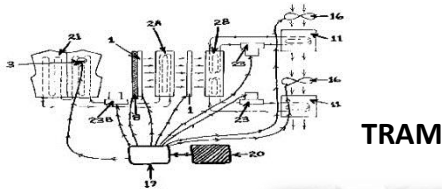


## e-Enabled Aircraft Control Systems (CS)

### Airborne Network Cyber Security Issues



## Airport Lighting and Monitoring Control System (ALMCS)



## Baggage Handling System (BHS)



## Avionics - Wireless



## Electronic Flight Bag (EFB)/iPad





# Example: identifying vulnerabilities in automobiles



Volpe Center Cyber Security Lab



# DHS/NIST framework for cyber security & cyber resilience reviews

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Voluntary Framework

## Cyber Resilience Review

1. Asset Management
2. Configuration & Change Management
3. Risk Management
4. Controls Management
5. Vulnerability Management
6. Incident Management
7. Service Continuity Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

# Cyber Security Evaluation Tool (CSET)

Assesses cybersecurity programs against standards & recommendations



Aviation



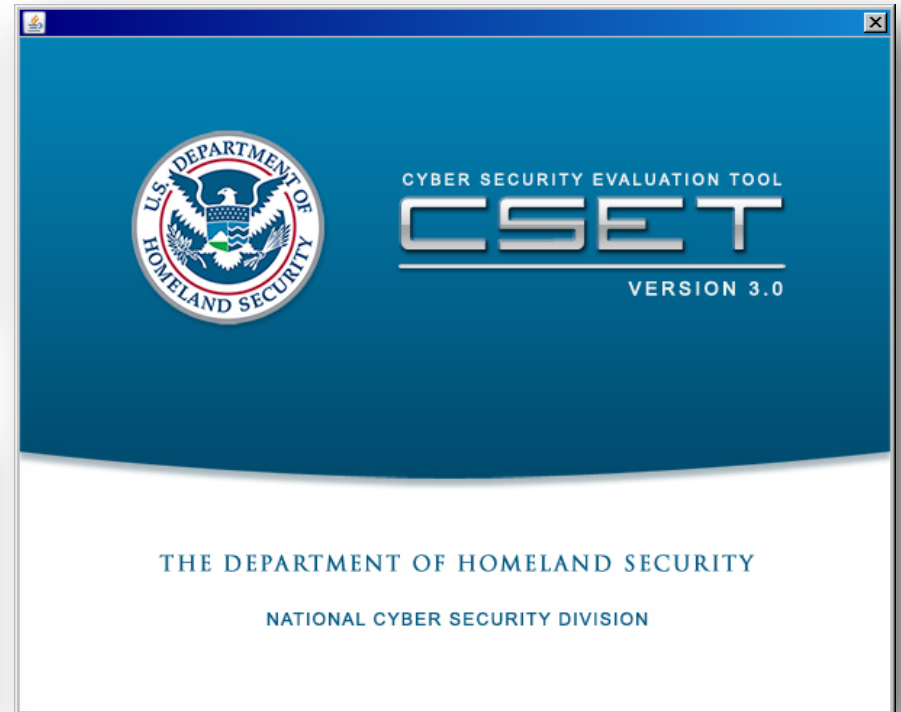
Pipeline



Maritime



Highway

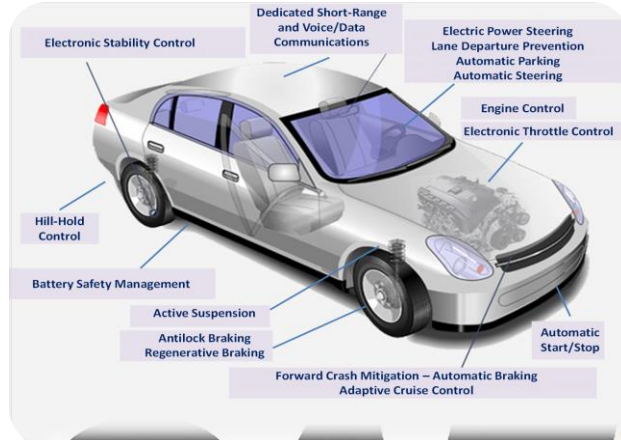


# How can the risks be mitigated?



**RTCA**

THE GOLD STANDARD FOR AVIATION SINCE 1935



**SAE**



AMERICAN  
PUBLIC  
TRANSPORTATION  
ASSOCIATION

Recommended practices

# How do we create awareness?



STOP | THINK  
CONNECT™



Smokey the Cybear

S O S

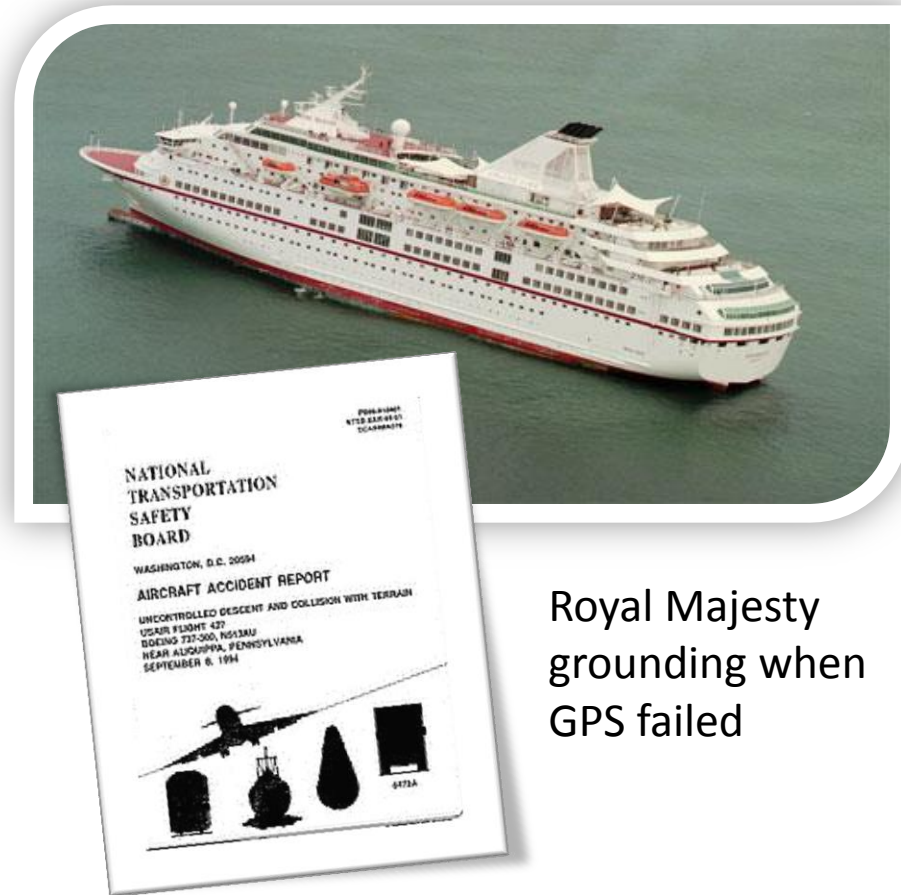
Save Our Systems



# Need to address human systems integration

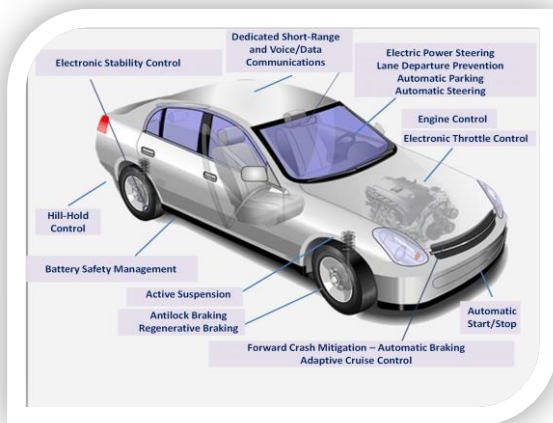
How do we recognize system failures and/or attacks?

Do we have “down time procedures”?

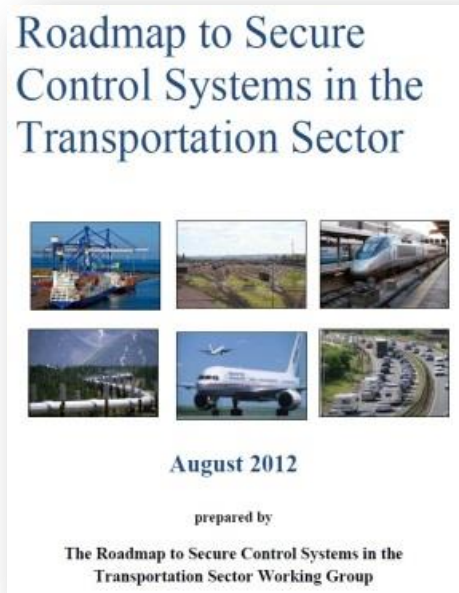


Royal Majesty grounding when GPS failed

# How do we respond to threats?



# What should the maritime community do to develop & implement a cyber security strategy?



**Assess overall risk & resilience**

- **Identify vulnerabilities**
- **Develop and evaluate controls**
- **Compile recommended practices**
- **Develop training for maritime IT & control systems**
- **Develop and exercise response capabilities**

# Michael Dinning

U.S. Department of Transportation

John A. Volpe National Transportation Systems Center

55 Broadway, Cambridge, MA 02142

[michael.dinning@dot.gov](mailto:michael.dinning@dot.gov)

617-494-2422 (w)

617-694-7518 (m)

The ideas in this briefing are the personal thoughts of the author, not the United States Department of Transportation.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear solely to illustrate the concepts presented in the briefing.